Remarks

Claims 1 to 44 are rejected.

Claims 1 to 44 remain in the application. Claims 1, 2, 5-7, 14, 15, 17-19, 26-30, 32-35 and, 42-44 have been amended.

Specifically, claims 1, 2, 5-7, 14, 15, 17-19, 27, 29, 30, 33, and 34 have been amended in order to avoid invoking 35 U.S.C. 112, sixth paragraph. In particular, all instances of phrases such as --the steps of-- have been deleted. Applicant wishes to note for the record that the amendments are neither narrowing, nor are the amendments being made for a reason substantially related to patentability. Applicant respectfully submits that no new matter has been added in the amendments.

Claim 35 has been amended for clerical reasons. Amended claim 35 now ends with a period.

Claim 1 has been amended to overcome the informality described by Examiner. Specifically, amended claim 1 now includes the word "and".

Claims 26 and 42 have been amended. Specifically, after the word "useable" the word "from" has been replaced with the word "form" as per the objection raised by Examiner.

For enhanced clarity the phrase "key-server" has been changed to "other than central key-server" when not referring to the central key-server in amended independent claim 27 and its dependent claims 28, 32-34 and 42-44 to ensure proper antecedence.

Claims 27-37 and 39-44 have been rejected under U.S.C. 102(b) as being anticipated by US patent #5,761,306 by Lewis, filed: 22 Feb 1996 (Lewis). Independent claim 27 has been amended to comprise, "when the portable data storage device is in communication with the computer and the other than central key-server is other than available, authenticating the individual for access to at least one of the secure data and secure keys stored on the portable storage data device". In the prior art of Lewis, the computer (node, Fig 1, item 12) is in communication with an insecure network and the central key server (Fig. 1, item 16) is clearly also in communication with the user node. Thus, amended claim 27 is no longer anticipated by Lewis. Referring to a passage from Lewis beginning at Col 6, line 66:

> *"Since network 10 is deemed insecure, it is assumed that if user node 1 requests a public key from user node 2, eavesdropper 18 could stand in place of user node 2, intercept the request, reply with a key known to eavesdropper 18, intercept the message and decrypt the message. To prevent this scenario, the user nodes supply their public keys to server 16 using a message which could not have been sent from eavesdropper 18 and which is not readable by eavesdropper 18."*

The prior art of Lewis does not suggest or support authenticating a user of a computer (node) while both the central key server and "data key storage" (Lewis, Column 5, line 33 and Fig. 1, item 20) are other than available therefore amended claim 27 in not obvious in light of Lewis.

Claims 28-37 and 39-44 depend either directly or indirectly from amended claim 27. Since amended claim 27 is neither anticipated nor obvious, claim 28-37 and 39-44 are not anticipated nor obvious.

Claim 38 has been rejected under U.S.C. 103(a) as being obvious in light of the combination of Lewis and US patent #6,219,439 filed: 9 July 1999 (Burger). As described hereinabove, the prior art of Lewis does not render amended independent claim 27 obvious. Since claim 38 depends from amended independent claim 27, claim 38 cannot be obvious in light of Lewis.

The prior art of Burger provides a system of authentication that works absent any key-server. The prior art of Burger does not suggest a method of authenticating a user comprising: "when the portable data storage device is in communication with the computer and the other than central key-server is other than available, authenticating the individual for access to at least one of the secure data and secure keys stored on the portable storage data device" as recited in amended claim 27. Specifically, as stated in Burger, column 4, lines 15 to 20,

> *"Another feature of the invention is that it is self-contained, portable, and in that regard, does not rely on communications with a remote location for authentication to be implemented. The invention provides a biometrics apparatus to authenticate the cardholder. In summary, the unit is a stand-alone unit and can be hand-held."*

Burger continues on column 4, line 34,

> *"The invention is a biometric authentication device which is preferably portable, hand-held and stand-alone, not relying upon a remote database and requires a plurality of inputs in order to authenticate the user."*

Thus, it is clear that the system according to Burger does not rely on a remote database in a process of authenticating the user. In fact, Burger clearly teaches away from their use. In contrast, the system according to the invention as recited in amended independent claim 27 does incorporate a central key-server and an other than central key-server. Therefore, it is apparent that the method of claim 27 is contrary to and, thus, not obvious in light of Burger. Claim 38 depends from claim 27 and, therefore, claim 38 cannot be obvious in light Burger.

An advantage of the method supported by dependent claim 27, is described in the present application, page 12 beginning on line 13,

> *"When cryptographic functions are performed within the portable storage devices 44, the secure keys are not available outside the portable storage devices 44. Since most cryptographic functions are performed on the portable storage devices 44, the key-server can support the processing of cryptographic functions for those individuals with forgotten portable storage devices 44. If a secure path is initiated between portable storage devices 44 and the key-server 41, then the keys stored within the two media are not available for capture or compromise".*

Neither Lewis nor Burger suggests the above stated advantage of such a load sharing system or method in which both the key servers and the portable storage devices handle authentication operations. It is strongly believed that a person of ordinary skill in the art would not arrive at such an advantage merely having reviewed Lewis and Burger. With this in mind it is apparent that the method according to amended independent claim 27 has an unforeseen advantage that is not present in the prior art of Lewis in combination with Burger. Therefore, amended independent claim 27 is not obvious in light of the combination of Lewis and Burger. Claim 38 depends from amended independent claim 27

and therefore is not obvious in light of Lewis in combination with Burger.

The method according to the invention, as recited in amended independent claim 27, clearly states, "...when the portable data storage device is in communication with the computer, determining the availability of an other than central key-server in communication with the computer..." As described with reference to arguments presented hereinbefore with regards to Burger's lack of incorporation of a key server, this is clearly contrary to the prior art of Burger. In contrast, Lewis features a "node public key database" (see Fig. 1 of Lewis) that supports many user nodes (see description of said figure in Lewis, column 5, lines 27 to 29). Thus, it is apparent that Burger teaches away from authenticating operations incorporating the use of remote servers that hold sensitive information as taught, for example, in the prior art of Lewis. With this in mind, it is highly unclear what motivation a person of ordinary skill in the art would have to combine the prior art of Lewis and Burger.

Based upon the aforestated lack of motivation to combine it is apparent that amended independent claim 27 is not obvious in light of the combination of Lewis and Burger. Further, the reduced demand for access to key servers in an advantageous, unforeseen result that is not taught by either Lewis or Burger and would not be apparent to one of ordinary skill in the art having reviewed the prior art of Lewis and Burger. Additionally, Burger teaches away from the use of key-servers, a necessary component used in carrying out the method of amended independent claim 27. Thus, it is apparent that claim 27 is not obvious in light of the combination of Burger and Lewis and therefore, claim 38, which depends from claim 27, cannot be obvious in light of Burger in combination with Lewis.

Claims 1-26 have been rejected under U.S.C. 103(a) as being obvious in light of the

combination of Lewis and US patent 6,611,850 by Shen, filed 18 Aug. 1998 (Shen). Lewis describes key management methods in column 7 beginning on line 29. Specifically, Lewis recites, "Key server 16 accepts key replacement commands from central public key controller 26 which decide when to replace the active public key, Apu." Referring to Fig. 1 of Lewis, it is clear that the central public key controller (item 26) and the key server (item 16) communicate without communicating with user nodes 1 and 2 (item 12). Clearly, the central key server (Fig. 1, item 26) is fixed. Lewis does not suggest that the central key server supports "a plurality of portable data storage devices each having stored thereon security data relating to a single authorized user" as recited in claim 1. Thus, it is apparent that independent claim 1 is not obvious given the prior art of Lewis.

As stated by Examiner with regards to independent claim 14, "Lewis does not explicitly state that this method (referring to copying form the key-server to the portable data storage device) of communicating keys between a key server and a plurality of portable storage devices is for the purpose of backup of the data of the key server." Therefore, independent claim 14 is not obvious based upon the prior art of Lewis.

Shen describes methods and apparatus of backing up data. Referring to Shen column 11, lines 19 to 41.

> *"Also, in FIG. 1, the original file hard disk 106 and backup file hard disk 110 that corresponds to the first and second storage devices respectively are indicated, but it does not limit the hard disk to be two; it can be one or more than three. The reason is because, in this invention, using the expression "a file stored in the first storage device is copied to the second storage device to make a backup file," could mean that, when a backup copy is being generated, it may merely be copied onto a different area of the same hard disk, from where the original file was stored. Furthermore, in FIG. 1, hard disks such as the original file hard disk 108 and backup file hard disk 110 is mentioned as an example of the storage medium, but*

the storage medium is not limited to a hard disk, but could be a floppy diskette, IC card, silicone disk and any other media that can be read/written from/to.

Furthermore, the computer 100 as in FIG. 1 is not limited to a desktop PC, but could be a notebook type PC. If in case the computer 100 is a notebook type PC, then the backup file hard disk could be connected, for example, via PC-Card (f/k/a Personal Computer Memory Card International Association ("PCMCIA") or printer port to a file server on the network (Ethernet) and use the file server as a backup file hard disk 110."

Clearly, Shen is merely indicating that any form of computer storage device is potentially useable for the file backup and restoration system according to Shen. Shen does not suggest any advantages for backing up data to any particular form of media. Indeed, Shen is vaguely suggesting that any media storage device is optionally incorporated. It should be noted that Shen does not address security concerns beyond mentioning that files are optionally encrypted. The system according to Shen is not specifically designed for supporting high security applications and Shen does not suggest a method of restoring encryption keys. Instead, referring to Disclosure of Invention of Shen, column 3, line 6:

"The backup/restore method as descried in this invention is a backup/restore method consisting of, (1) a "backup copy generating process" where a random file stored in the first storage device is copied to a second storage device to make a backup copy, and (2) a "restore process" where such backup copy generated by the above-mentioned "backup copy generating process" is used to restore (an) existing file(s) or (a) non-existing (i.e., already deleted) file(s) in the first storage device, and (3) a "restore detail instructing process" where the target file (file name) and time period is designated to execute the above-mentioned "restore process" to restore those file(s) to a state of designated time period backing from the current

time, and (4) a "restore control process" where, in case a "restore process" is executed during the above-mentioned "restore detail instructing process," one file that meets the designated "file name" and "time period" criteria is selected and control the execution of the above-mentioned "restore process.""

The methods according to the invention as recited in claims 1 and 14 are not intended to restore "random files" as recited by Shen (column 3, line 6). Shen is providing a system for providing a backup of a presumably very large quantity of data in which the data is not particularly secure. A person of skill in the art of key database management would not be drawn to a prior art reference for restoring "random files" when tasked with providing a system for restoring a key data to a key server. Thus, it is apparent that the invention as recited in claim 1 is not obvious in light of Shen. Claims 2-13 depend from claim 1 and since claim 1 is not obvious claims 2-13 cannot be obvious in light of Shen.

Similarly, independent claim 14 includes: "providing the key-server". Shen does not suggest providing a key server and therefore independent claim 14 is not obvious in light of Shen. Claims 15 to 26 depend from claim 14 and since claim 14 is not obvious in light of Shen, claim 15 to 26 cannot be obvious in light of Shen.

A person of ordinary skill in the art tasked with providing a system for restoring keys to a key server having read both Lewis and Shen would be lead to a prior art method of backing up keys. Specifically, Lewis suggests managing public keys from a central public key controller that is in data communication with the key server. Shen suggests restoring data from a medium that has the data. The problem in combining them is that Lewis is very security oriented whereas Shen is not. A person tasked with providing a system to provide a backup of key data would likely go to substantial length to ensure that the key data remain very secure. Thus, when the person of ordinary skill in the art would likely consider Fig. 1 or Lewis and, having reviewed the prior art of Shen, decide to provide a

backup node public key database having a data communication link with the central public key controller for the purpose of restoring the node public key database (Lewis, Fig. 1, item 24). Further, a person of skill in the art of key database management would not be drawn to a prior art reference for storing "random files" (Shen, column 3, line 6) when tasked with providing a system for restoring a key server and thus it is not apparent that a person of ordinary skill in the art would see any motivation to combine Lewis and Shen. Thus, it is apparent that a person of skill in the art would have no motivation to combine Lewis and Shen in a way that would provide an inventive device. Thus, the combination of the two prior art references does not suggest an advantage in restoring data from "a plurality of portable data storage devices each having stored thereon security data relating to a single authorized user" as recited in independent claim 1. Therefore, it is clear that the combination of Lewis and Shen would not lead a person of ordinary skill in the art to the invention as recited in independent claim 1. Additionally, the combination of prior art references would not lead a person of ordinary skill in the art to: "copying from the key-server to the portable data storage device, security data relating to the authorized user for use by the specific authorized user in accessing data within the network" in the context of backing up the key server as recited in independent claim 14. Thus, independent claim 14 is not obvious in light of the combination of Lewis and Shen.

Claims 2 to 13 depend from independent claim 1 and since independent claim 1 is not obvious in light of the combination of Lewis and Shen, claims 2 to 13 cannot be obvious in light of the same combination. Similarly, claims 15 to 26 depend from independent claim 14 which is not obvious in light of the combination of the Lewis and Shen and therefore claims 15 to 26 cannot be obvious in light of the combination of Lewis and Shen.

No new matter has been added.

A Petition for Extension of Time is filed concurrently with this response.

Please charge any additional fees required or credit any overpayment to Deposit Account No. 50-1142.

Applicant requests favourable reconsideration of the amended application.

Respectfully,

Gordon Freedman, Reg. No. 41,553

Freedman and Associates
117 Centrepointe Drive, Suite 350
Nepean, Ontario
K2G 5X3 Canada

Tel (613) 274-7272
Fax (613) 274-7414
Email: info@ipatent4u.com

VL/sah